



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/576,565	04/05/2007	Kiyoshi Iwata	062453	4127
38834	7590	11/03/2008	EXAMINER	
WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP			CHAI, LONGBIT	
1250 CONNECTICUT AVENUE, NW				
SUITE 700			ART UNIT	PAPER NUMBER
WASHINGTON, DC 20036			2431	
			MAIL DATE	DELIVERY MODE
			11/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/576,565	IWATA, KIYOSHI	
	Examiner	Art Unit	
	LONGBIT CHAI	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 April 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) 2 and 8 is/are allowed.
- 6) Claim(s) 1, 3-7 and 9-11 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 05 April 2007 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>4/20/2006</u> | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 4/5/2007 but is a 371 case of PCT/JP04/15493 application filed on 10/20/2004 and has a foreign priority application filed on 10/20/2003.

Specification

The abstract of the disclosure is objected to because the total number of words should not be exceeding 150 words within the abstract section. Correction is required. See MPEP § 608.01(b).

Claim Objections

2. Claim 1 is objected to because of the following informalities: “firstly decrypting bit data of original information such as plaintext” should be replaced with “firstly encrypting bit data of original information such as plaintext” because it make more sense to encrypt original information such as plaintext rather than to decrypt such a plaintext information. Appropriate correction(s) is (are) required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.
3. Please correct “bite” as “bit” across each of the claims.

Art Unit: 2431

4. Claim 10 is objected to because of the following informalities: “an valid person” should be replaced with “an authenticated person”.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1 and 3 – 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uyama (U.S. Patent 2002/0126848), in view of Klonowski et al. (U.S. Patent 5,479,514).

As per claim 1, Uyama teaches an information encrypting transmission and reception method in an information transmission and reception network composed of a plurality of senders and receivers having computers being connected and communicating each other via a web network and a data center having a server computer for receiving electronic key data of bit data formed by the senders and receivers and personal data such as address corresponding to each electronic key data to register the server computer and certifying the senders and the receivers with each personal data (Uyama: Para [0125]: personal data such as electronic key associated with a sender or a receiver is registered at the server), comprising:

by one of the senders, firstly encrypting bit data of original information such as plaintext to be transmitted to one of the receivers by performing an exclusive OR operation in use of the bit data of the registered electronic key of the sender and transmitting the firstly encrypted data attached with personal data of the sender and the receiver to the receiver (Uyama: Para [0014] Line 1 – 3, pare [0016] Line 9 – 14, Para [0178] Line 5 – 6 and Para [0184]: (a) the encryption key as part of the enciphering program can be designated by a transmitter (i.e. the sender) and (b) both of the encryption / decryption methods can be XOR).

However, Uyama does not disclose expressly by the server computer of the data center, decrypting the bit data of the electronic key of the sender by performing an exclusive OR operation on the transmitted firstly encrypted bit data in use of bit data of the key data of the sender certified with the personal data of the sender, secondly encrypting the decrypted data by performing an exclusive OR operation the in use of bit data of the registered electronic key of the receiver certified with transmitted personal data of the receiver so as to form secondly encrypted bit data, and transmitting the secondly encrypted bit data to the receiver.

Klonowski teaches by the server computer of the data center, decrypting the bit data of the electronic key of the sender by performing an exclusive OR operation on the transmitted firstly encrypted bit data in use of bit data of the key data of the sender certified with the personal data of the sender, secondly encrypting the decrypted data by performing an exclusive OR operation the in use of bit data of the registered electronic key of the receiver certified with transmitted personal data of the receiver so as to form

secondly encrypted bit data, and transmitting the secondly encrypted bit data to the receiver (Klonowski: Column 2 Line 56 – 59 & Uyama: Para [0178] Line 5 – 6 and Para [0184]: (a) Klonowski teaches, in view of a set of connected nodes (including the sender, receiver and intermediate routers or servers), any node on the routing path can first decrypt the message that was encrypted by the sender and then re-encrypted with a new key (i.e. known to the downstream node) – i.e. a receiver (b) the encryption / decryption methods can be XOR, as taught by (Uyama: Para [0178] Line 5 – 6 and Para [0184]), the (encrypted message) XOR (sender key) is indeed simply the decryption of the encrypted message and re-encrypt the clear message using the XOR (receiver key)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Klonowski within the system of Uyama because (a) Uyama teaches providing a system of protected communication enabling a highly safe communication over the network (Uyama: Para [0004]), and (b) Klonowski teaches an secure data communication method by allowing encrypted communication throughout a properly designed network, while at the same time avoiding the necessity of sharing encryption keys with independent vendor nodes and avoiding key proliferation prevalent in other networks (Klonowski: Column 1 Line 60 – 67).

by the receiver, receiving the secondly encrypted bit data from the data center, and decrypting the secondly encrypted bit data in to the original information such as plaintext by performing an exclusive OR operation in use of bit data of the electronic key of the receiver (Klonowski: Column 2 Line 56 – 59 & Uyama: Para [0178] Line 5 – 6 and

Para [0184]: Klonowski teaches, in view of a set of connected nodes (including the sender, receiver and intermediate routers or servers), any node on the routing path can first decrypt the message that was encrypted by the sender and then re-encrypted with a new key (i.e. known to the downstream node) – i.e. a receiver can then decrypt the encrypted message by using the receiver key that is also known to the adjacent upstream node (i.e. the server)).

As per claim 3, Uyama teaches the original information such as plaintext is preliminary encrypted by performing an exclusive OR operation on at least each bite of the original information in use of random number bit data in advance of firstly encrypting of the original data in use of bit data of the electronic key of the sender (Uyama: Para [0161], Para [0178] Line 5 – 6 and Para [0184]: multiple encryption technique to enhance data security).

As per claim 4, Uyama teaches bit data of the random number and/or electronic key is a password random number of the n bit including 6 to 10 digits of 64 bits, a pseudo random number based on the random number, a chaos random number, or a fractal random number (Uyama: Para [0178]: Both enciphering and deciphering can be realized as the XOR per 1,024 bits of the key sentence and the digital data – i.e. the random data).

As per claim 5, Uyama teaches the server computer of the data center uses electronic key data set by each sender and receiver as electronic personal seal data for authentication and as information hiding data for hiding data transmitted and received between the sender and the receiver (Uyama: Para [0171] Line 10: the enciphering key corresponding to each person as information hiding data).

As per claim 6, Uyama teaches chaos image data or fractal image data is used for the electronic personal seal data and/or the information hiding data (Para [0178]): Both enciphering and deciphering can be realized as the XOR per 1,024 bits of the key sentence and the digital data – i.e. the digital image data (e.g., a sentence of a PDF file)).

As per claim 7, Uyama teaches the image data in claim 6 is moving image data (Para [0024] and [0025]: a suitable automatic change of the application order data according to a pre-set rule – i.e. for example, various methods such as, a change based on the `date`, `frequency of use`, or based on an identification code designated by the transmitter).

6. Claims 9 – 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uyama (U.S. Patent 2002/0126848), in view of Sehr (U.S. Patent 2001/0018660).

As per claim 9, Uyama teaches an information encrypting transmission and reception method, comprising:

forming firstly encrypted data (C) by performing an exclusive OR operation on bit data (A) of original information such as plaintext to be transmitted in use of random bit data (B) known to a sender and a receiver (Uyama: Para [0014] Line 1 – 3, pare [0016] Line 9 – 14, Para [0178] Line 5 – 6 and Para [0184]: (a) the encryption key as part of the enciphering program can be designated by a transmitter (i.e. the sender) and (b) both of the encryption / decryption methods can be XOR and (c) an enciphering key is indeed a random bit data);

forming secondly encrypted data (E) by performing an exclusive OR operation on the data (C) in use of bit data (D) of an electronic key obtained only by the sender and receiver (Uyama: Para [0161], Para [0178] Line 5 – 6 and Para [0184]: multiple encryption technique to enhance data security is also disclosed by Uyama).

However Uyama does not disclose expressly forming thirdly encrypted data (G) by performing an exclusive OR operation on the data (E) in use of bit data (F) of an electronic envelop registered by the sender or the receiver; and transmitting the thirdly encrypted data (G) and the data (F) of the electronic envelop to the receiver.

Sehr teaches forming thirdly encrypted data (G) by performing an exclusive OR operation on the data (E) in use of bit data (F) of an electronic envelop registered by the sender or the receiver (Sehr: Para [0115] Line 13 – 19 & Uyama: Para [0178] Line 5 – 6 and Para [0184]: Sehr teaches (a) the public key (i.e. envelop key) can include, for example, an unique mailing address – i.e. the addressee on the envelop (as an envelop

key) (b) a sender can communicate secure messages to a receiver while encrypting the messages with the public key (i.e. envelop key) of that receiver prior to transmission and (c) only the addressee on the envelop can open the envelop and read the letter – using the envelop key); and

transmitting the thirdly encrypted data (G) and the data (F) of the electronic envelop to the receiver (Sehr: Para [0115] Line 13 – 19: the envelop key (i.e. an unique mailing address) is indeed the addressee on the envelop (as an envelop key)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sehr within the system of Uyama because (a) Uyama teaches providing a system of protected communication enabling a highly safe communication over the network (Uyama: Para [0004]), and (b) Sehr teaches an secure data communication method to guarantee a secure information exchange and to authenticate a cryptography scheme based system data (Sehr: Para [0115]).

As per claim 10, Uyama as modified teaches bit data of the random number, bit data of the electronic key, and bit data of the electronic envelop are registered to the data center or the server computer set as an authenticator so as to be readable only by an valid person (Uyama: Para [0171] Line 10: the enciphering key corresponding to each person as information hiding data).

As per claim 11, Uyama as modified teaches bit data of the random number and/or electronic key is a password random number of the n bit including 6 to 10 digits of 64 bits, a pseudo random number based on the random number, a chaos random number, or a fractal random number (Uyama: Para [0178]: Both enciphering and deciphering can be realized as the XOR per 1,024 bits of the key sentence and the digital data – i.e. the random data).

Allowable Subject Matter

Claims 2 and 8 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: in an information encrypting transmission and reception system, wherein by the sender server computer, receiving bit data of the electronic key of the receiver by submitting personal data of the receiver to the data center, secondly encrypting the firstly encrypted bit data by performing exclusive OR operation in use of received bit data of the electronic key of the receiver, and transmitting the secondly encrypted bit data attached with personal data of the sender and the receiver to the receiver server computer; and further by the receiver server computer, receiving the secondly encrypted bit data, receiving bit data of the electronic key of the sender by submitting personal data of the sender to the data center, thirdly encrypting the secondly encrypted bit data by performing exclusive OR operation in use of received bit data of the

electronic key of the sender, and informing the receiver about the reception of the thirdly encrypted bit data or transmitting the thirdly encrypted bit data to the receiver.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2431
09/16/2008